INsite Security

There are three aspects to INsite security:

1. Limiting what functions can be performed.
2. Limiting client access.
3. Limiting access to reports.

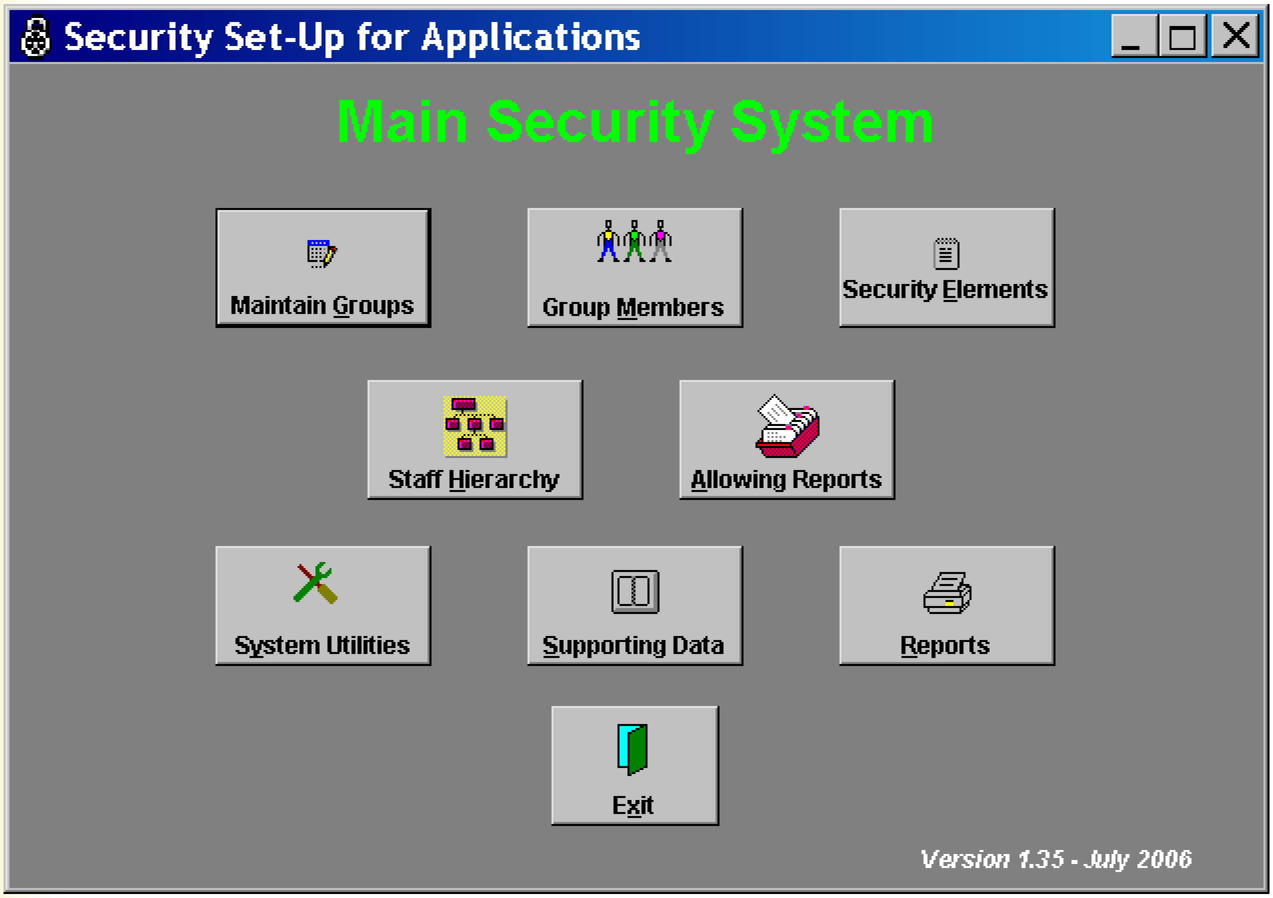
Logging in and getting started

The INsite Security module can be launched by clicking on 

in the INsite folder.

You will need to log in to the module. This login is not the same as your INsite login name and password. The default Security module login ID is Supervisor and the default password is xxxx. You will want to change the password to restrict access to the Security module.

The following screen will appear:



To set up users for the Security Module or to change user passwords click on 'System Utilities'.

Then click on 'Add/Maintain Users'. The following screen will appear:

To change the password choose the user from the Operator list and type in the new password in the 'password' box. The Level indicates how much access the user will have within the Security Module. Users who need to perform most functions in the Security module should have access level '9'.

The password has to be at least 4 characters.

Click 'Save new Password' and Exit.

To add a new user, click 'Add a New Operator' . A box will appear, type in the user name and hit the 'Enter' key. The user name will then be at the top of the page. Enter a password, assign a level, and click 'Save new Password'. You can then exit.

You will need to exit the Security module for password and user changes to go into effect.

Limiting what functions can be performed

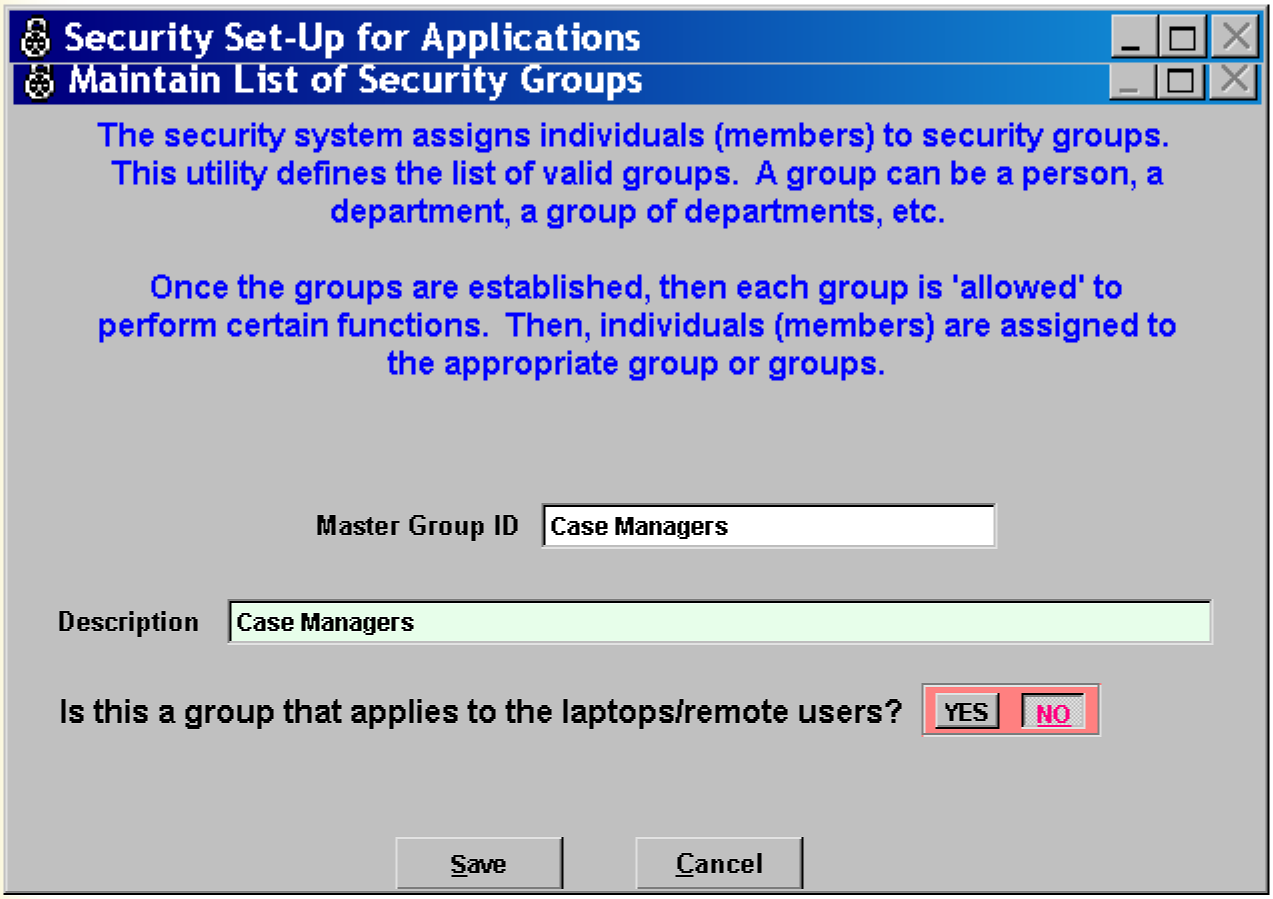
Nearly every button/function in INsite is controlled by Security. Users of INsite should be defined by their role i.e. does this user mostly do Client Processing such as a case manager or are they a Supervisor who does other things besides Client Processing tasks.

Those roles are referred to as security '**groups**' in the Security module. Each group can be assigned the individual functions that they need to use in INsite -- these are referred to as the security '**elements**'.

Setting up a group in the Security Module

Click on Supporting Data >> Master List of Groups.

To add a new group, click 'Add'.



Type in the Name/ID for the group.

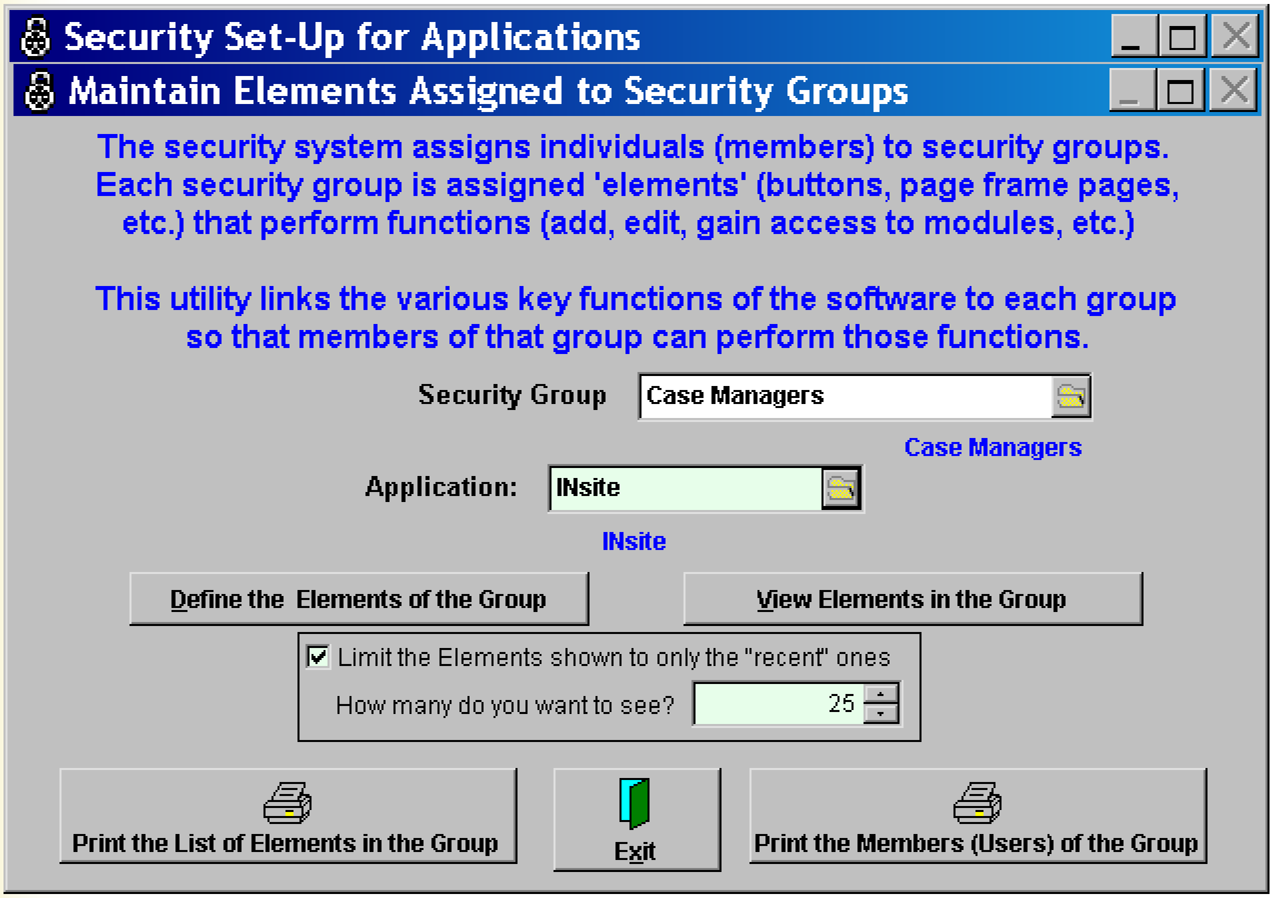
Type in a description for the group.

You will also need to indicate whether or not this group will be used on remote systems.

Click 'Save'.

Assigning functions (elements) to the group

Now that you have a new group, you will need to assign specific functions\elements to that group. To do so, click on 'Maintain Groups'. The following screen will appear:



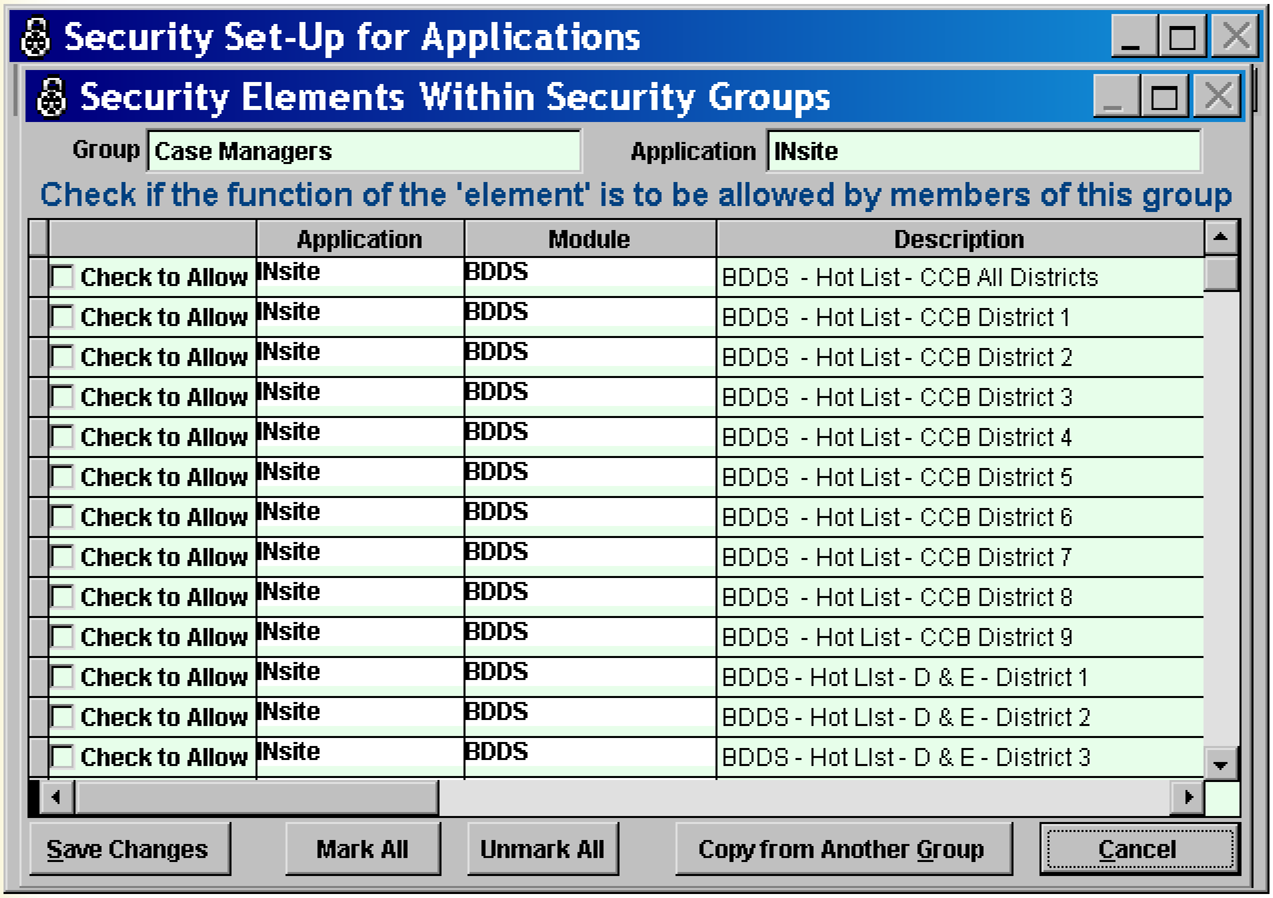
Choose the Security Group to which you want to assign functions.

Choose the Application (INsite)

If you want to only assign new elements (when new functions are added to INsite), you change the number of elements in the list by clicking the "Limit the Elements shown to only the 'recent' ones" box and indicate how many you want to see.

If you are setting up a new group, uncheck the "Limit the Elements shown to only the 'recent' ones".

Then click 'Define the Elements of the Group'. The following screen appears:



	Application	Module	Description
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB All Districts
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 1
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 2
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 3
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 4
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 5
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 6
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 7
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 8
Check to Allow	INsite	BDDS	BDDS - Hot List - CCB District 9
Check to Allow	INsite	BDDS	BDDS - Hot LIst - D & E - District 1
Check to Allow	INsite	BDDS	BDDS - Hot LIst - D & E - District 2
Check to Allow	INsite	BDDS	BDDS - Hot LIst - D & E - District 3

This list all the elements available in the program.

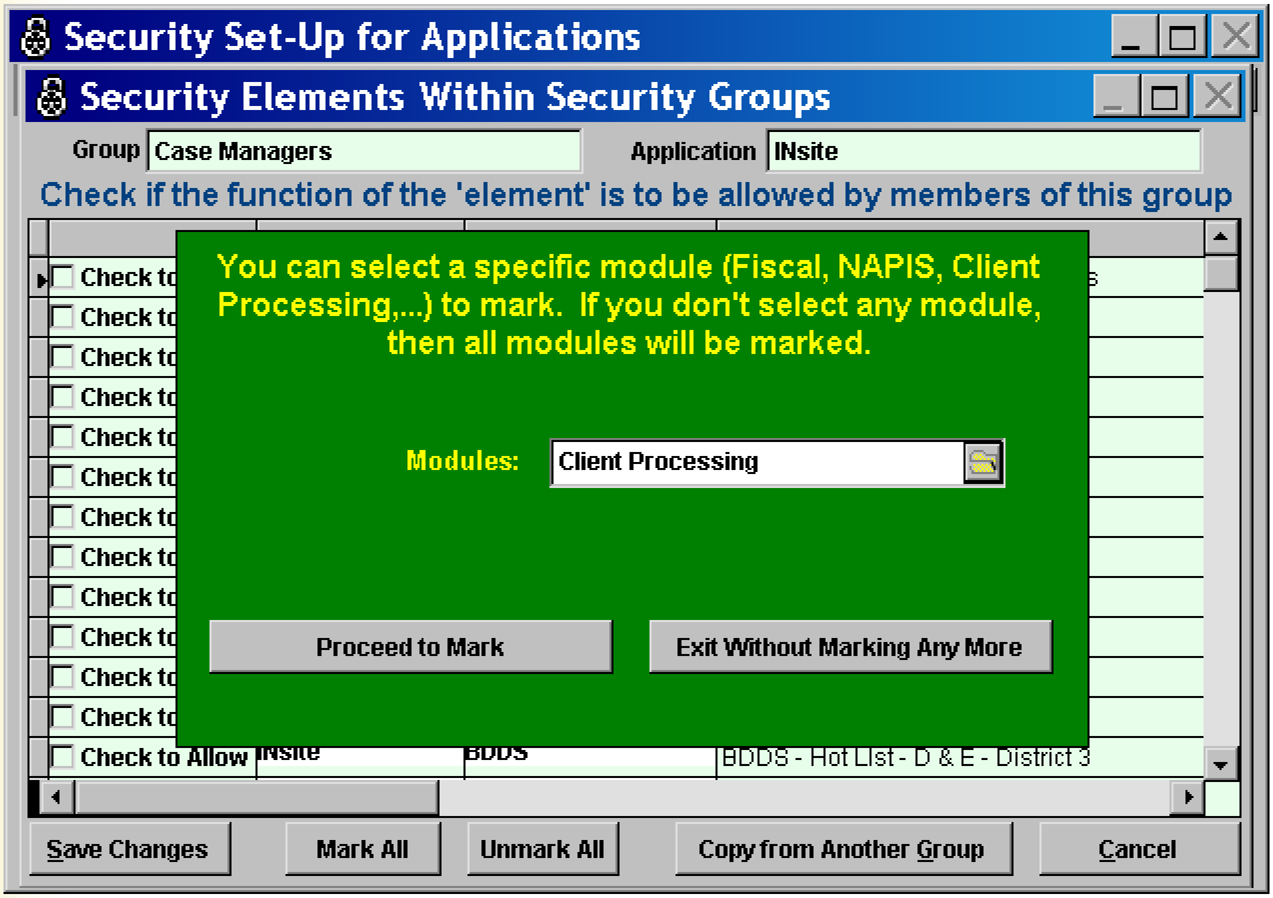
Column one indicates if this group is allowed this function.

Column two shows the application (INsite)

Column three shows the Module: the elements are divided into categories (modules) based upon their functioning such as Client Processing, Import, Export, and Main Menu.

The fourth column is a short description of the function.

You can mark all the elements in one module by clicking 'Mark All'. The following screen will appear:



Select the module for which you want to mark all elements. Then click 'Proceed to Mark'.

If there is another module for which you want to mark all elements, select it and click 'Proceed to Mark'.

When you have marked all for the desired modules, click 'Exit Without Marking Any More'.

To mark all elements for every module, leave the Modules box blank and click 'Proceed to Mark'. You will receive a message asking you to confirm that you want to mark everything. Say 'Yes'.

Once you are back on the page that shows all the elements, you can then selectively mark or un-mark elements.

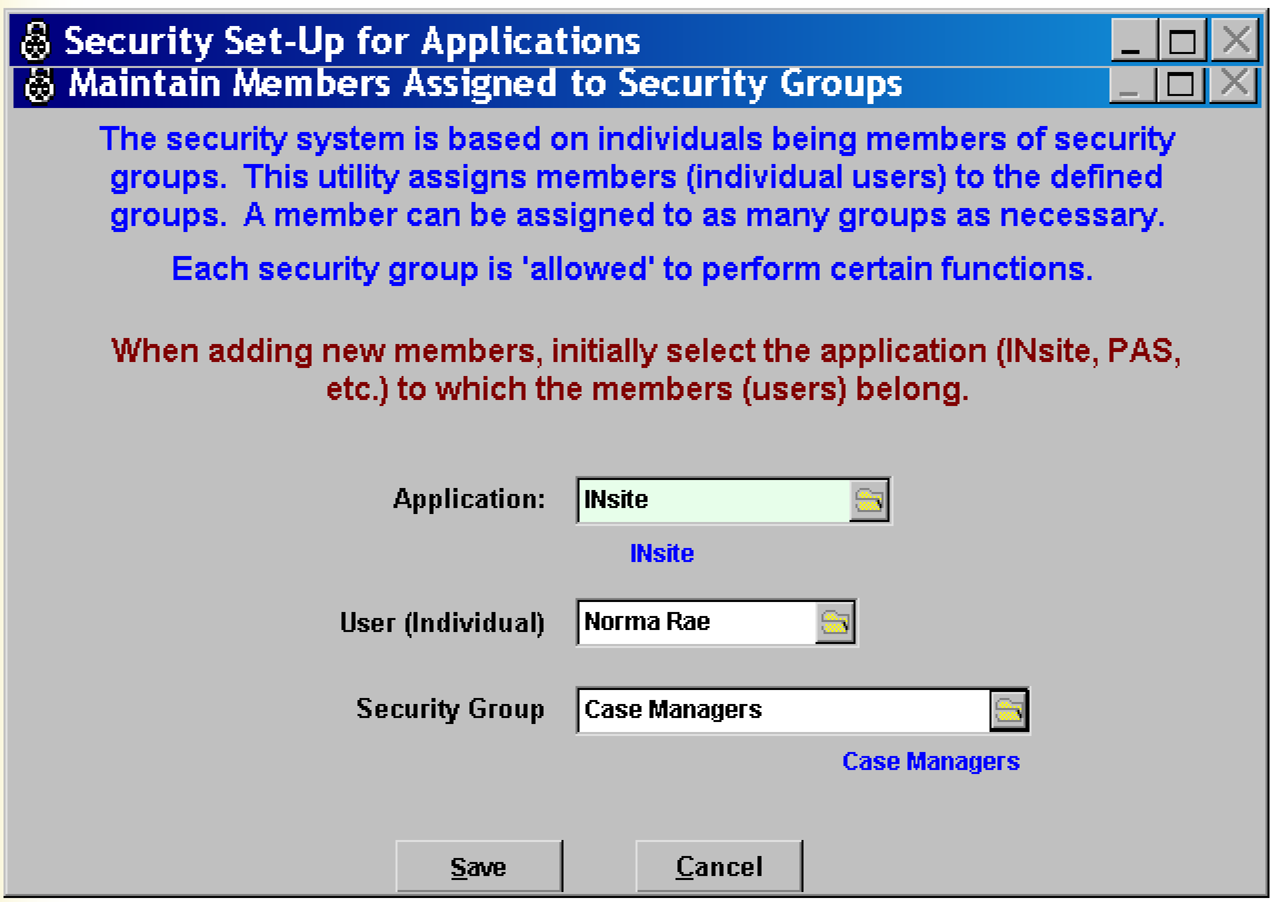
For example, if you want the Case Manager group to have access to everything in the Client Processing module, you could use the Mark All button to mark all of them and then you can selectively un-check items that you do not want to the case managers to have access to in Client Processing--such as supervisory review of CCB's. Just scroll down the list until you get to the items that say 'Client Processing' in the module column. Find the specific element you want to un-check by looking at the 'Description' column, for example, 'Client Processing - CCB - CCB Reviewed by Office '. Then un-check that item in the first column.

Note: be sure to give access to the needed buttons on the INsite main screen by checking the appropriate items in the 'Main Menu' module.

When you have marked the items, click 'Save Changes'.

Assigning Users to Groups

Once you have set up groups and assigned elements to those groups, you need to assign each INsite user to a group. To do this click on 'Group Members'. Click 'Add'.



Select the application (INsite).

Select the INsite user from the list.

Choose a Security Group for that user.

Click 'Save'.

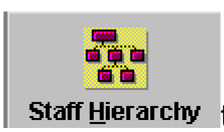
In this example, the user Norma Rae is assigned to the Case Managers group. When she logs into INsite, she will be able to do only those things that have been assigned to the Case Managers group.

You can assign an INsite user to multiple security groups if they have multiple roles within the company.

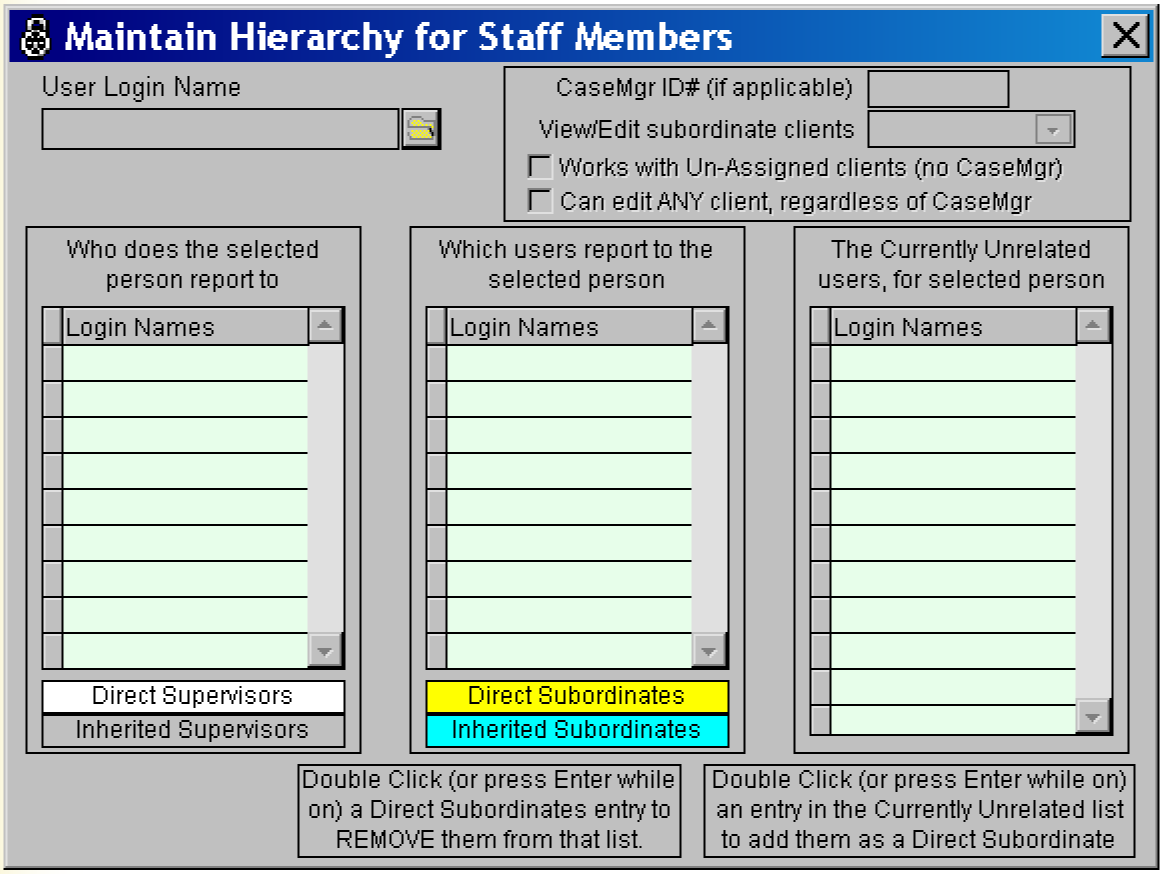
Limiting client access

Please note: the features to limit client access and the ability to restrict reports is not available unless you go to System Utilities in the Security Module, click on Reindex Tables, and click 'Build' next to 'CaseMgr#+LoginName Xref & Staff Hierarchy. Once these tables are built, you will need to set up the users according to the following instructions or no one will be able to access any clients. So if you have a lot of users you may want set aside some time when no one will be needing to access consumers in Client Processing.

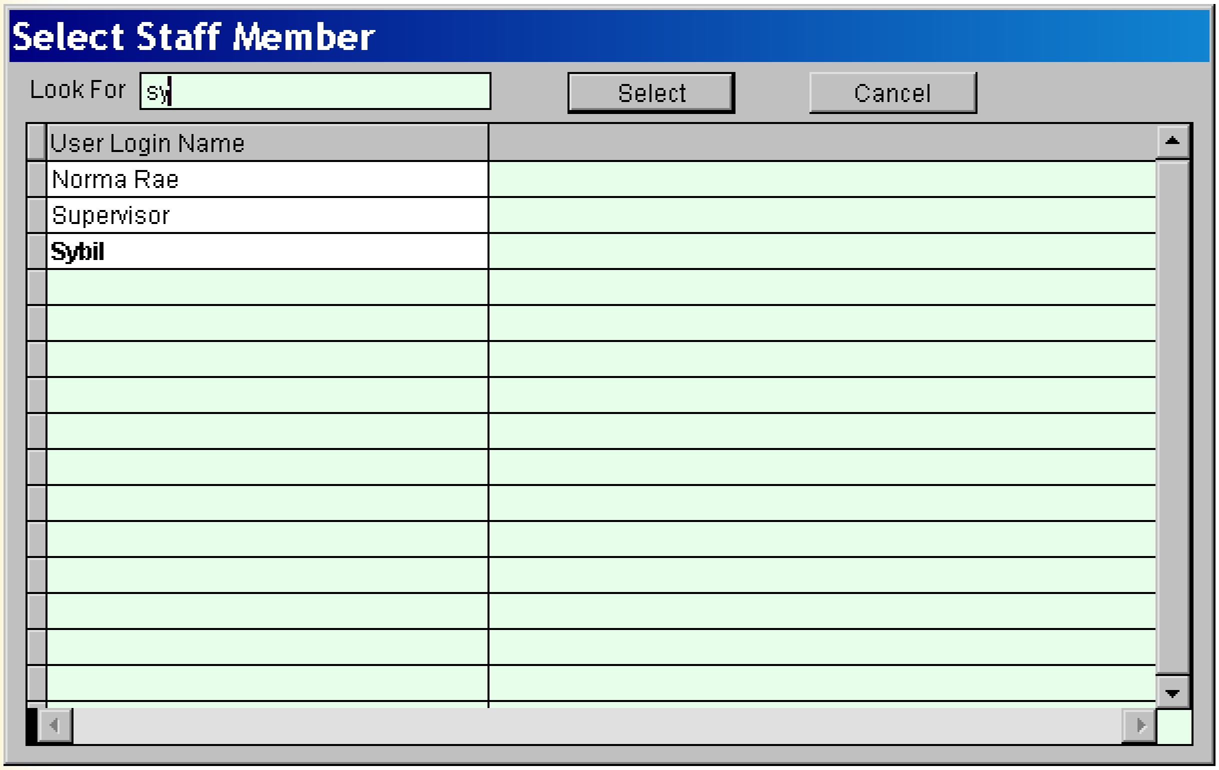
To restrict access to client information in Client Processing, you will need to set up the Staff Hierarchy. Note the restriction only applies to viewing client info in Client Processing. Other modules such as Nutrition, Fiscal, and NAPIS are not affected.

Click 

to access the hierarchy setup screen:

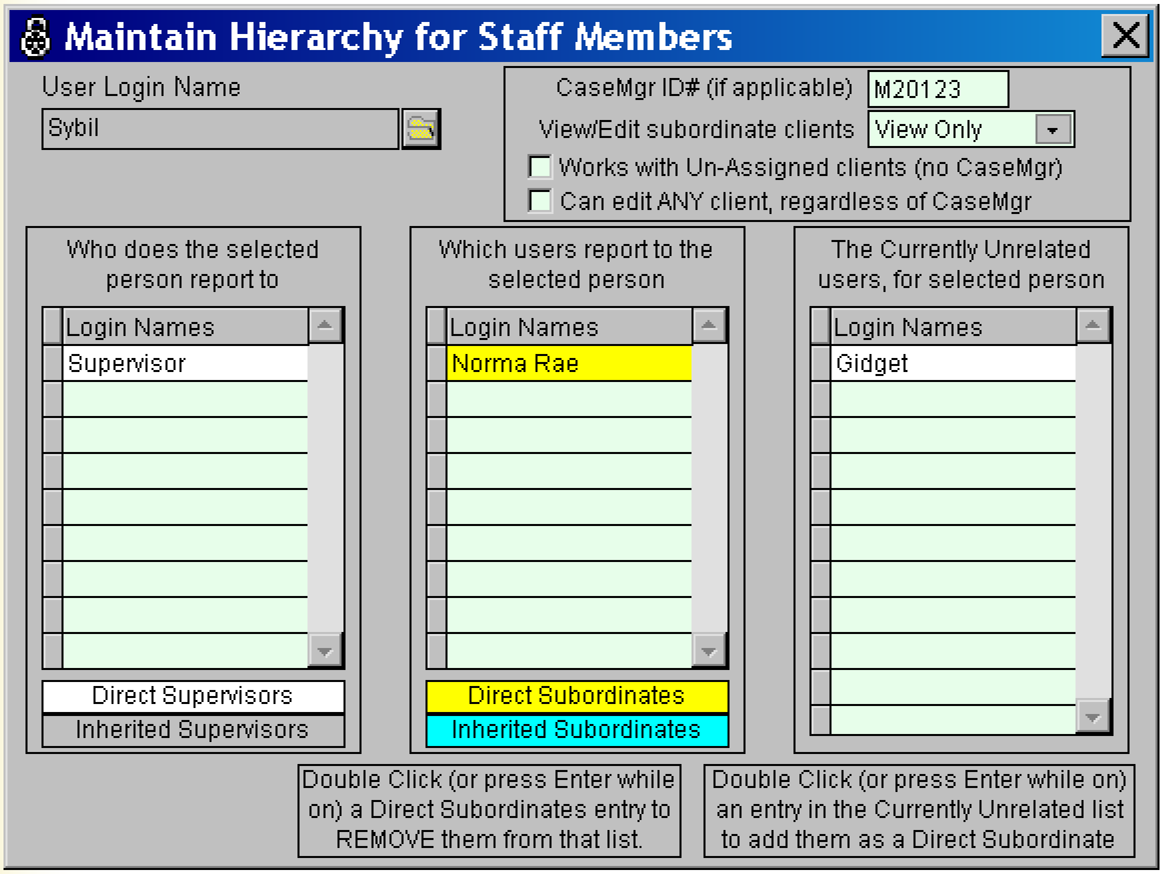


Choose an INsite User by clicking the folder in the "User Login Name" box. The following screen will appear:



Type in the"Look For' box to find a specific user in the list. When you are on the user you want, click 'Select'

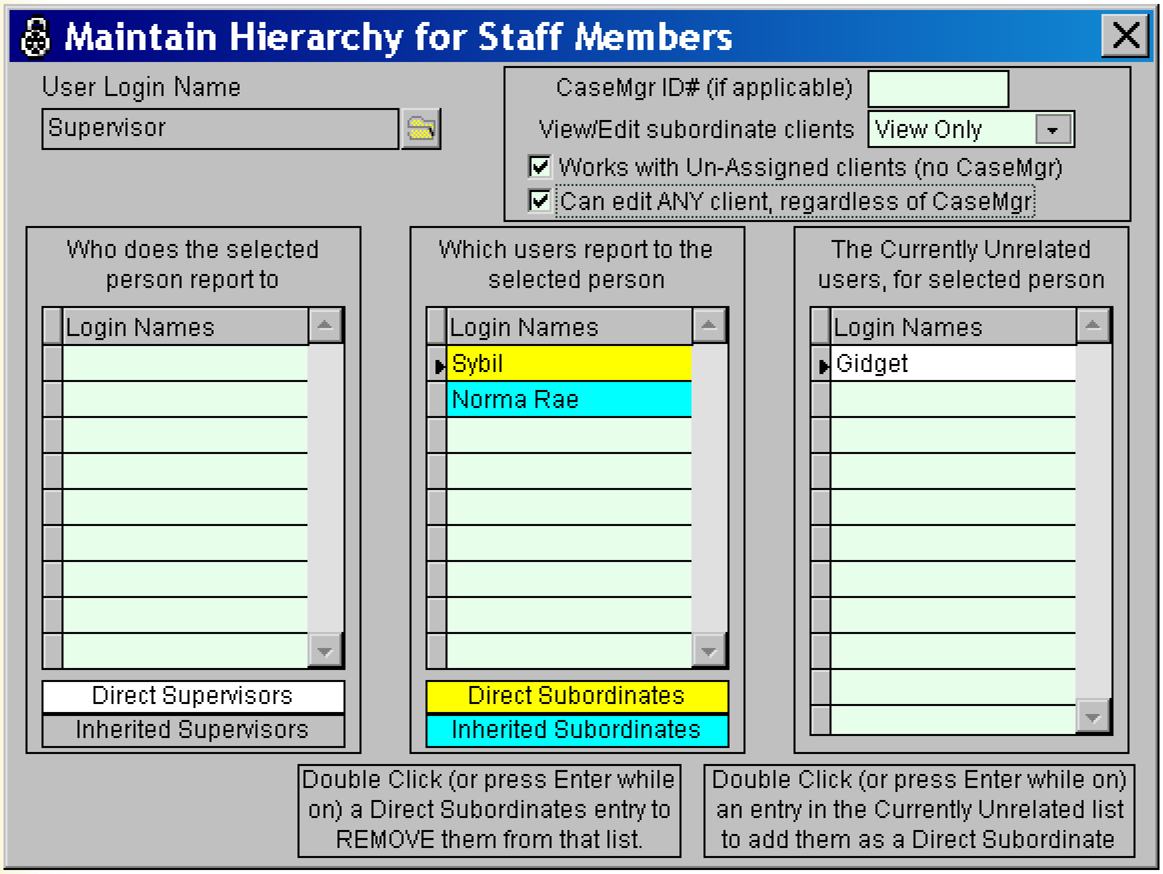
After selecting a user, you will need to indicate what users report to them.



In Example 1, the INsite user selected is Sybil. She has already been assigned to be a subordinate to the user Supervisor. By double-clicking any of the users in the third column, the user will be moved to the second column, making them a subordinate of Sybil. So Sybil reports to Supervisor and Norma Rae reports to Sybil. Gidget does not have any relationship to Sybil.

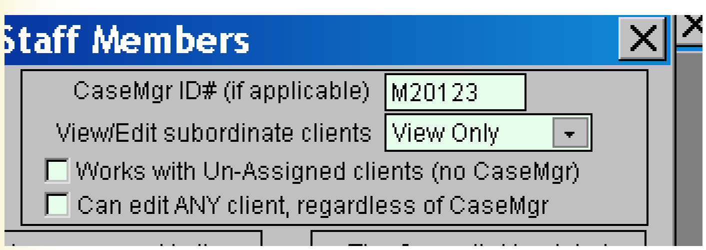
To remove a 'subordinate', double-click the person's loging name in the center list. Only direct subordinates can be removed; inherited entries must be removed by taking them out of the list for their direct supervisor.

Following is the setup information for the user Supervisor:



Example 2 shows that Supervisor does not report to anybody and Sybil reports to Supervisor directly while Norma Rae reports to Supervisor because she reports to Sybil. Gidget does not have any relationship to Supervisor.

Other options that can be set for a user:



<u>Link User to their Case Manager ID Number</u>

You can fill in a CM ID # for a user if they have one. They will then be allowed to see all consumers assigned to that case manager on the INsite demographics screen. Any user that this user reports to will also have access to this user's consumers.

In Example 1, the user Sybil has a Case Manager ID # M20123. So she will have access to all clients in Client Processing and Local Hot Lists assigned to that CM number. Because she reports to the user Supervisor, Supervisor will also have access to her consumers. However, the user Norma Rae will not have access to Sybil's consumers.

In Example 2, the user Supervisor does not have a Case Manager ID but will have access to Sybil and Norma Rae's consumers if they have a CM Number entered.

<u>Determine if the User can edit or only view clients of subordinate users</u>

There are three options for Users who have other users that report to them in terms of the level of access they have to their subordinates' consumers:

1. Full Rights --changes can be made
2. View Only -- they can only look at the information
3. No Access -- they do not have access at all

In example 1, Sybil can only view Norma Rae's consumers.

In example 2, Supervisor can edit Sybil and Norma Rae's consumers.

<u>Allow the user to work with clients that do not have a CM assigned</u>

There may be consumers in INsite that do not have a case manager assigned yet. These consumers will be inaccessible to anyone if there are no users given this ability.

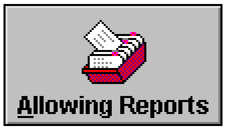
Example 2 shows Supervisor as having the ability to work with clients that do not have a CM assigned.

<u>Allow full access to all clients regardless of CM</u>

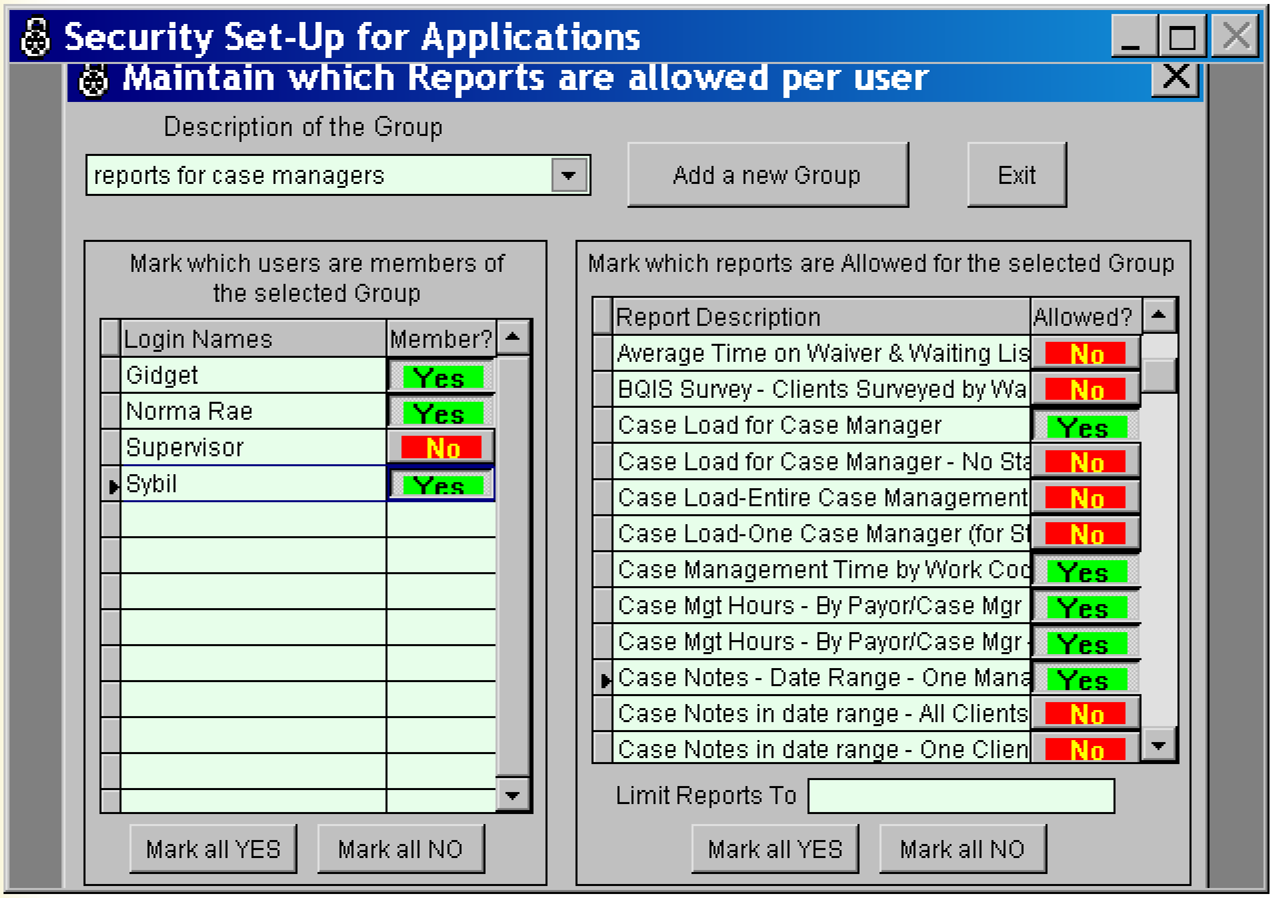
Check this option sparingly and for only those people in the agency that need to have access to all clients.

Limiting access to reports

Since reports will generally have the potential to contain information for all consumers in the system, this feature will allow you to determine which users can run which reports.

Click on 

. The following screen will appear:



Click 'Add a new Group' to set up a new report group. You will receive a box in which you can type the name of your group.

On the left side of the screen are the INsite users. Click the button next to the user you want to be in the group. If you want all users to be in the group click "Mark all YES'.

On the right side is the list of reports, click the button to indicate which reports you want this group to be able to run. You can search for a particular report by using the 'Limit Reports To' feature. You can also use the 'Mark all YES' button to assign all reports. If you have limited the list and use the 'Mark All' feature, only the items in the list will be marked.

Click 'Exit' to save changes and go back to the security main screen.